AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (currently amended) A computer-implemented method for controlling access to a resource of a plurality of resources, the method comprising the steps of:

    creating and storing in a filesystem of an Operating System a plurality of files that each represents [[the]] a different resource of the plurality of resources;

    assigning an access value to a file attribute of a file that represents the resource, wherein the file attribute is used by the Operating System to manage file access, wherein the access value corresponds to a combination of a particular role and the resource;

    receiving user-identifying information from a user requesting access to the resource, wherein the user-identifying information comprises a role associated with the user, wherein the role is determined from a user identifier uniquely associated with the user and from a group identifier associated with a group that includes the user;

    receiving a resource identifier associated with the resource;

    creating an access identifier based on the user-identifying information and the resource identifier, wherein the access identifier is formatted as a file attribute that is used by the Operating System to manage file access;

    calling the Operating System to perform a file operation on the file, wherein calling the Operating System includes [[by]] providing the access identifier to the Operating System to attempt access to the file; and

granting the user access to the resource only when the Operating System call successfully

performs the file operation, wherein the Operating System call successfully

performs the file operation if the access identifier matches the access value;

wherein the file operation on the file representing the resource is selected from a group

consisting of opening the file, closing the file, deleting the file, reading from the

file, writing to the file, executing the file, appending to the file, reading a file

attribute, and writing a file attribute.

2.   (original) A method as recited in Claim 1, wherein the access identifier comprises:

a first set of bits for storing a role identifier, wherein the role identifier is associated with

the role; and

a second set of bits for storing the resource identifier.

3.   (original) A method as recited in Claim 1, wherein:

the step of creating an access identifier based on the user-identifying information and the

resource identifier comprises formatting the access identifier as a group identifier

file attribute; and

the step of calling the Operating System to perform an operation on the file representing

the resource comprises:

assigning the access identifier to a group identifier attribute of an

Operating System process; and

calling an Operating System routine from the Operating System process to

perform the operation on the file representing the resource.

4.   (original) A method as recited in Claim 1, wherein the step of calling the Operating

System to perform an operation on the file representing the resource comprises

comparing the access identifier to an identifier included in an Access Control List file

attribute associated with the file representing the resource, wherein the Access Control

List file attribute includes the identifiers of all users and all groups of users allowed to

access the file representing the resource.

5.   (canceled)

6.   (previously presented) A method as recited in Claim 1, the method further comprising the

steps of:

reading a permission bit associated with the file representing the resource, wherein the

        permission bit corresponds to the operation performable on the file representing

        the resource;

based on the operation on the file indicated by the permission bit, determining a resource

        operation that is performable on the resource; and

granting the user the privilege of performing the resource operation on the resource only

        when the permission bit allows the operation to be performed on the file

        representing the resource.

7.   (previously presented) A method as recited in Claim 1, the method further comprising the

steps of:

opening the file representing the resource;

reading from the file representing the resource a permission indicator associated with a

resource operation; and

enabling the user to perform the resource operation on the resource only when the

permission indicator indicates that the user is allowed to perform the resource

operation on the resource.

8.   (canceled)

9.   (currently amended) A method as recited in Claim [[8]] 1, wherein the file attribute used

by the Operating System to manage file access is a group identifier file attribute.

10.   (currently amended) A computer-implemented method for controlling access to a

resource of a plurality of resources, the method comprising the steps of:

assigning an access value to a group identifier file attribute of a file that represents the

resource, wherein the group identifier file attribute is used by the Operating

System to manage file access, wherein the access value is uniquely determined by

a combination of a particular role and the resource;

receiving a user identifier from a user requesting access to the resource, wherein the user

identifier is uniquely associated with the user;

receiving a group identifier associated with a group to which the user belongs;

based on the user identifier and the group identifier, determining a role associated with

the user, wherein a role identifier is uniquely associated with the role;

receiving a resource identifier associated with the resource, wherein [[the]] each resource

of the plurality of resources is represented by a different file stored in a filesystem

of an Operating System;

constructing an access identifier on the basis of the role identifier and the resource

identifier, wherein the access identifier conforms to the format of a group

identifier file attribute that is used by the Operating System to manage file access;

making an Operating System call to perform a file operation on the file representing the

resource, wherein the Operating System call uses the access identifier to gain

access to the file representing the resource; and

granting the user access to the resource only when the Operating System call successfully

performs the file operation on the file representing the resource, wherein the

Operating System call successfully performs the file operation if the access

identifier matches the access value;

wherein the file operation on the file representing the resource is selected from a group

consisting of opening the file, closing the file, deleting the file, reading from the

file, writing to the file, executing the file, appending to the file, reading a file

attribute, and writing a file attribute.

11.   (original) A method as recited in Claim 10, wherein the access identifier comprises:

a first set of bits for storing the role identifier, wherein the role identifier represents a

bitmap, each bit of the bitmap uniquely associated with a role of the user; and

a second set of bits for storing the resource identifier.

12.   (previously presented) A method as recited in Claim 10, wherein the step of making an

Operating System call to perform an operation on the file representing the resource

comprises:

storing the group identifier value of a group identifier attribute of an Operating System

                process;

assigning the access identifier to the group identifier attribute of the Operating System

                process;

calling an Operating System routine from the Operating System process to perform the

                operation on the file representing the resource, wherein the operation on the file

                representing the resource is performed only when the value of the group identifier

                attribute of the Operating System process matches the value of the group

                identifier file attribute of the file representing the resource; and

resetting the group identifier attribute of the Operating System process to the stored

                group identifier value.

13.   (original) A method as recited in Claim 10, wherein the step of making an Operating

System call to perform an operation on the file representing the resource comprises

comparing the access identifier to an identifier included in an Access Control List file

attribute associated with the file representing the resource, wherein the Access Control

List file attribute includes the identifiers of all users and all groups of users allowed to

access the file representing the resource.

14.   (canceled)

Ser. No. 10/698,498 filed October 30, 2003
Sanjay Aiyagari et al. – GAU 2161 (Kim)
Docket No. 50325-0805

15.   (previously presented) A method as recited in Claim 10, the method further comprising

the steps of:

reading a permission bit associated with the file representing the resource, wherein the

        permission bit corresponds to a file operation performable on the file representing

        the resource;

based on the file operation indicated by the permission bit, determining a resource

        operation that is performable on the resource; and

granting the user the privilege of performing the resource operation on the resource only

        when the permission bit allows the file operation to be performed on the file

        representing the resource.

16.   (previously presented) A method as recited in Claim 10, the method further comprising

the steps of:

opening the file representing the resource;

reading from the file representing the resource a permission indicator associated with a

        resource operation; and

granting the user the privilege of performing the resource operation on the resource only

        when the permission indicator indicates that the user is allowed to perform the

        resource operation on the resource.

17.   (canceled)

18.   (currently amended) A system for controlling access to a resource, of a plurality of

resources, connected to a network, the system comprising:

Seq. No. 7841   8

a client host capable of accessing the resource in response to a request for access from a

user;

one or more processors executing an Operating System, wherein the Operating System

operatively controls a filesystem that includes a number of files; and

a computer readable medium having stored therein an Application Programming

Interface, wherein the Application Programming Interface is logically interposed

between the client host and the Operating System and comprises one or more

routines including routines which, when executed by the one or more processors,

cause the one or more processors to perform the steps of:

creating and storing in the filesystem a <u>plurality of</u> file<u>s</u> that <u>each</u> represents

[[the]] <u>a different</u> resource <u>of the plurality of resources</u>;

<u>assigning an access value to a file attribute of a file that represents the resource,</u>

<u>wherein the file attribute is used by the Operating System to manage file</u>

<u>access, wherein the access value corresponds to a combination of a</u>

<u>particular role and the resource;</u>

receiving user-identifying information from the user requesting access to the

resource, wherein the user-identifying information comprises a role

associated with the user, wherein the role is determined from a user

identifier uniquely associated with the user and from a group identifier

associated with a group that includes the user;

receiving a resource identifier associated with the resource;

creating an access identifier based on the user-identifying information and the

resource identifier, wherein the access identifier is formatted as a file

attribute that is used by the Operating System to manage file access;

calling the Operating System to perform a file operation on the file, wherein

calling the Operating System includes [[by]] providing the access

identifier to the Operating System to attempt access to the file; and

granting the user access to the resource only when the Operating System call

successfully performs the file operation, wherein the Operating System

call successfully performs the file operation if the access identifier

matches the access value;

wherein the file operation on the file representing the resource is selected from a

group consisting of opening the file, closing the file, deleting the file,

reading from the file, writing to the file, executing the file, appending to

the file, reading a file attribute, and writing a file attribute.

19.   (original) A system as recited in Claim 18, wherein the access identifier comprises:

a first set of bits for storing a role identifier, wherein the role identifier is associated with

the role; and

a second set of bits for storing the resource identifier.

20.   (original) A system as recited in Claim 18, wherein:

the step of creating an access identifier based on the user-identifying information and the

resource identifier comprises formatting the access identifier as a group identifier

file attribute; and

the step of calling the Operating System to perform an operation on the file representing

the resource comprises:

assigning the access identifier to a group identifier attribute of an Operating

System process; and

calling an Operating System routine from the Operating System process to

perform the operation on the file representing the resource.

21-38.   (canceled)

39.   (currently amended) A computer-readable storage medium, for controlling access to a

resource of a plurality of resources, carrying one or more sequences of instructions

which, when executed by one or more processors, causes the one or more processors to

perform the steps of:

creating and storing in a filesystem of an Operating System a plurality of files that each

represents [[the]] a different resource of the plurality of resources;

assigning an access value to a file attribute of a file that represents the resource, wherein

the file attribute is used by the Operating System to manage file access, wherein

the access value corresponds to a combination of a particular role and the

resource;

receiving user-identifying information from a user requesting access to the resource,

wherein the user-identifying information comprises a role associated with the

user, wherein the role is determined from a user identifier uniquely associated

with the user and from a group identifier associated with a group that includes the

user;

receiving a resource identifier associated with the resource;

creating an access identifier based on the user-identifying information and the resource

identifier, wherein the access identifier is formatted as a file attribute that is used

by the Operating System to manage file access;

calling the Operating System to perform a file operation on the file, wherein calling the

Operating System includes [[by]] providing the access identifier to the Operating

System to attempt access to the file; and

granting the user access to the resource only when the Operating System call successfully

performs the file operation, wherein the Operating System call successfully

performs the file operation if the access identifier matches the access value;

wherein the file operation on the file representing the resource is selected from a group

consisting of opening the file, closing the file, deleting the file, reading from the

file, writing to the file, executing the file, appending to the file, reading a file

attribute, and writing a file attribute.

40.   (previously presented) A computer-readable storage medium as recited in Claim 39,

wherein the access identifier comprises:

a first set of bits for storing a role identifier, wherein the role identifier is associated with

the role; and

a second set of bits for storing the resource identifier.

41.   (previously presented) A computer-readable storage medium as recited in Claim 39,

wherein:

the step of creating an access identifier based on the user-identifying information and the

resource identifier comprises formatting the access identifier as a group identifier

file attribute; and

the step of calling the Operating System to perform an operation on the file representing

the resource comprises:

assigning the access identifier to a group identifier attribute of an

Operating System process; and

calling an Operating System routine from the Operating System process to

perform the operation on the file representing the resource.

42.   (previously presented) A computer-readable storage medium as recited in Claim 39,

wherein the step of calling the Operating System to perform an operation on the file

representing the resource comprises comparing the access identifier to an identifier

included in an Access Control List file attribute associated with the file representing the

resource, wherein the Access Control List file attribute includes the identifiers of all users

and all groups of users allowed to access the file representing the resource.

43.   (canceled)

44.   (previously presented) A computer-readable storage medium as recited in Claim 39,

carrying one or more additional sequences of instructions which, when executed by one

or more processors, further causes the one or more processors to perform the steps of:

reading a permission bit associated with the file representing the resource, wherein the

permission bit corresponds to a file operation performable on the file representing

the resource;

based on the file operation indicated by the permission bit, determining a resource

operation that is performable on the resource; and

granting the user the privilege of performing the resource operation on the resource only

when the permission bit allows the file operation to be performed on the file

representing the resource.

45.   (previously presented) A computer-readable storage medium as recited in Claim 39,

carrying one or more additional sequences of instructions which, when executed by one

or more processors, further causes the one or more processors to perform the steps of:

opening the file representing the resource;

reading from the file representing the resource a permission indicator associated with a

resource operation; and

enabling the user to perform the resource operation on the resource only when the

permission indicator indicates that the user is allowed to perform the resource

operation on the resource.

46.   (canceled)

47.   (currently amended) A computer-readable storage medium as recited in Claim [[46]] 39,

wherein the file attribute used by the Operating System to manage file access is a group

identifier file attribute.

48.   (currently amended) A computer-readable storage medium, for controlling access to a

resource of a plurality of resources, carrying one or more sequences of instructions

which, when executed by one or more processors, causes the one or more processors to

perform the steps of:

assigning an access value to a group identifier file attribute of a file that represents the

    resource, wherein the group identifier file attribute is used by the Operating

    System to manage file access, wherein the access value is uniquely determined by

    a combination of a particular role and the resource;

receiving a user identifier from a user requesting access to the resource, wherein the user

    identifier is uniquely associated with the user;

receiving a group identifier associated with a group to which the user belongs;

based on the user identifier and the group identifier, determining a role associated with

    the user, wherein a role identifier is uniquely associated with the role;

receiving a resource identifier associated with the resource, wherein [[the]] each resource

    of the plurality of resources is represented by a different file stored in a filesystem

    of an Operating System;

constructing an access identifier on the basis of the role identifier and the resource

    identifier, wherein the access identifier conforms to the format of a group

    identifier file attribute that is used by the Operating System to manage file access;

making an Operating System call to perform a file operation on the file representing the

    resource, wherein the Operating System call uses the access identifier to gain

    access to the file representing the resource; and

granting the user access to the resource only when the Operating System call successfully

performs the file operation on the file representing the resource, wherein the

Operating System call successfully performs the file operation if the access

identifier matches the access value;

wherein the file operation on the file representing the resource is selected from a group

consisting of opening the file, closing the file, deleting the file, reading from the

file, writing to the file, executing the file, appending to the file, reading a file

attribute, and writing a file attribute.

49.   (previously presented) A computer-readable storage medium as recited in Claim 48,

wherein the access identifier comprises:

a first set of bits for storing the role identifier, wherein the role identifier represents a

bitmap, each bit of the bitmap uniquely associated with a role of the user; and

a second set of bits for storing the resource identifier.

50.   (previously presented) A computer-readable storage medium as recited in Claim 48,

wherein the step of making an Operating System call to perform an operation on the file

representing the resource comprises:

storing the group identifier value of a group identifier attribute of an Operating System

process;

assigning the access identifier to the group identifier attribute of the Operating System

process;

calling an Operating System routine from the Operating System process to perform the

operation on the file representing the resource, wherein the operation on the file

representing the resource is performed only when the value of the group identifier

attribute of the Operating System process matches the value of the group

identifier file attribute of the file representing the resource; and

resetting the group identifier attribute of the Operating System process to the stored

group identifier value.

51.   (previously presented) A computer-readable storage medium as recited in Claim 48,

wherein the step of making an Operating System call to perform an operation on the file

representing the resource comprises comparing the access identifier to an identifier

included in an Access Control List file attribute associated with the file representing the

resource, wherein the Access Control List file attribute includes the identifiers of all users

and all groups of users allowed to access the file representing the resource.

52.   (canceled)

53.   (previously presented) A computer-readable storage medium as recited in Claim 48,

carrying one or more additional sequences of instructions which, when executed by one

or more processors, further causes the one or more processors to perform the steps of:

reading a permission bit associated with the file representing the resource, wherein the

permission bit corresponds to a file operation performable on the file representing

the resource;

based on the file operation indicated by the permission bit, determining a resource

operation that is performable on the resource; and

granting the user the privilege of performing the resource operation on the resource only

when the permission bit allows the file operation to be performed on the file

representing the resource.

54.   (previously presented) A computer-readable storage medium as recited in Claim 48,

carrying one or more additional sequences of instructions which, when executed by one

or more processors, further causes the one or more processors to perform the steps of:

opening the file representing the resource;

reading from the file representing the resource a permission indicator associated with a

    resource operation; and

granting the user the privilege of performing the resource operation on the resource only

    when the permission indicator indicates that the user is allowed to perform the

    resource operation on the resource.

55.   (canceled)

56.   (currently amended) An apparatus for controlling access to a resource of a plurality of

resources, comprising:

means for creating and storing in an Operating System filesystem a plurality of files that

    each represents [[the]] a different resource of the plurality of resources;

means for assigning an access value to a file attribute of a file that represents the

    resource, wherein the file attribute is used by the Operating System to manage file

    access, wherein the access value corresponds to a combination of a particular role

    and the resource;

means for receiving user-identifying information from a user requesting access to the

resource, wherein the user-identifying information comprises a role associated

with the user, wherein the role is determined from a user identifier uniquely

associated with the user and from a group identifier associated with a group that

includes the user;

means for receiving a resource identifier associated with the resource;

means for creating an access identifier based on the user-identifying information and the

resource identifier, wherein the access identifier is formatted as a file attribute that

is used by the Operating System to manage file access;

means for calling the Operating System to perform a file operation on the file, wherein

calling the Operating System includes [[by]] providing the access identifier to the

Operating System to attempt access to the file; and

means for granting the user access to the resource only when the Operating System call

successfully performs the file operation, wherein the Operating System call

successfully performs the file operation if the access identifier matches the access

value;

wherein the file operation on the file representing the resource is selected from a group

consisting of opening the file, closing the file, deleting the file, reading from the

file, writing to the file, executing the file, appending to the file, reading a file

attribute, and writing a file attribute.

57.   (previously presented) An apparatus as recited in Claim 56, wherein the access identifier

comprises:

a first set of bits for storing a role identifier, wherein the role identifier is associated with

the role; and

a second set of bits for storing the resource identifier.

58. (previously presented) An apparatus as recited in Claim 56, wherein:

means for creating an access identifier based on the user-identifying information and the

resource identifier comprises means for formatting the access identifier as a group

identifier file attribute; and

means for calling the Operating System to perform an operation on the file representing

the resource comprises:

means for assigning the access identifier to a group identifier attribute of

an Operating System process; and

means for calling an Operating System routine from the Operating System

process to perform the operation on the file representing the

resource.

59. (canceled)